PROBABLE PRIME PREDICAMENTS

Richard L. Francis

Southeast Missouri State University

Abstract. This article focuses on the concept of primality, a topic which extends from the dawn of history to the present. It likewise foreshadows some of the challenges confronting the mathematical world of the twenty-first century. Various tests of primality are often cumbersome or difficult to apply – including the Sieve of Eratosthenes and Wilson's Theorem. Other tests are typified by Fermat's Little Theorem. The notion of repunit numbers extends this pursuit and leads to the intriguing area of fraudulent primes. It likewise provides an interesting classroom activity in which converses and the expressing of necessary and sufficient conditions are analyzed.

1. Introduction. The challenge of the converse has played a critical role in the history of mathematics and has repeatedly given rise to the most appealing of questions. Such challenges span an impressive number of centuries and prove quite abundant in the more recent history. Included are the celebrated Euclid-Euler characterization of even perfect numbers, the Gaussian regular polygon constructibility standard, and the Steiner-Lehmus-Terquem Problem of angle bisectors. Prime numbers, a substantial part of Books VII, VIII, and IX of Euclid's *Elements*, have likewise provided extremely difficult questions as varying converses are analyzed. Among these extended modern day pursuits is the problem of false primes.

2. False Primes and Fermat's Little Theorem. Fermat's Little Theorem was formally conjectured in western culture by Fermat in 1640. Proved by Leonhard Euler in 1736, it reveals that if a is not divisible by a prime p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

That is, $a^{p-1} - 1$ is divisible by the prime number p provided a is not divisible by p [1]. The question of the validity of the converse, dating from perhaps as early as 500 B.C. in Oriental mathematics, naturally arose. Such a converse would provide a method of establishing the primality of a select positive integer. Not until the year 1819 was the matter finally resolved by the congruence discovery that

$$2^{340} \equiv 1 \pmod{341}.$$

Note that 341 is not prime, its factorization being (11)(31). Composite numbers x, satisfying $2^{x-1} \equiv 1 \pmod{x}$, are given the name "pseudoprimes to the base 2." Today, it is known that these numbers form an infinite set. Interestingly, if n is a pseudoprime to the base 2, so is $2^n - 1$. Such a construction guarantees the infinitude of the set [2]. It is also known that the arithmetic progression generated by $an + b$ where a and b are relatively prime produces an unending number of pseudoprimes. This powerful theorem is highly reminiscent of Dirichlet's Theorem concerning the generating of prime numbers. Several small pseudoprimes beyond 341 are the numbers 561, 645, 1105, and 1729.

Significantly, the encounter with pseudoprimes is relatively rare as the integers unfold. So seemingly infrequently does the converse to Fermat's Little Theorem fail that some regard it as an acceptable primality test for a number. It has recently been established that there are $882,206,716$ primes less than 20 billion, but merely $19,865$ pseudoprimes to the base 2. Such a mind-boggling count was obtained by the mathematicians John L. Selfridge, Jan Bohman, and Samuel S. Wagstaff [3]. A strong feeling exists that the Little Theorem of Fermat thus has a converse which rarely produces composites [4]. The word "rarely" has a connotation in this context somewhat at odds with that of conventional usage, especially as one notes that the set of pseudoprimes is an infinite set.

Though the set of pseudoprimes and the allied topics of Carmichael numbers have been the object of considerable study throughout the twentieth century [1], other areas of false prime encounters have not. As suggested, a false prime is one of relatively infrequent counterexamples to the converse of a theorem which requires primality in its hypothesis. Here a great departure from Wilson's Theorem is noted. Such a theorem provides a necessary and sufficient condition of primality [5], a feature lacking in some degree in Fermat's Little Theorem.

3. False Primes and Repunit Numbers. A repunit number, a term coined by Albert H. Beiler, is simply a positive integer consisting of all "ones" in its decimal representation. The symbol R_n will be used to denote the number which thus consists of n ones in its digital format. For any prime p greater than 5, it follows by Fermat's Little Theorem that p is a divisor of $10^{p-1} - 1$. More specifically, p is a divisor of $99999999\ldots999$ where

$p-1$ "nines" appear in the dividend, and consequently, p is a divisor of $11111111111\ldots111$. That is, for all primes p greater than 5, p is a divisor of R_{p-1}. For example, $7|R_6$, $43|R_{42}$, and $65537|R_{65536}$.

The question implicit in this theorem's development is again that of the converse. If $p|R_{p-1}$, does it follow that p is prime? Should the answer be "yes," then a simply described test for primality would follow. Should the answer be "no," then the matter of frequency of failure must be addressed (and thus, the probabilistic nature of this test for primality).

Composite numbers p which satisfy the condition $p|R_{p-1}$ are called "deceptive primes" [3]. However, do deceptive primes exist? Is it conceivable that the set of deceptive primes is empty in which case the above "test" for primality is fully valid? Consider the exploratory table below which tests all odd integers greater than 5 but less than 91. Note as well that the test does not fail even once in the listing.

A PROBABILISTIC TEST FOR PRIMALITY

x	Does x divide R_{x-1}?	Is x prime or composite?
7	yes	prime
9	no	composite
11	yes	prime
13	yes	prime
15	no	composite
17	yes	prime
19	yes	prime
21	no	composite
23	yes	prime
25	no	composite
27	no	composite
29	yes	prime
31	yes	prime
33	no	composite
35	no	composite
37	yes	prime
39	no	composite
41	yes	prime

43	yes	prime
45	no	composite
47	yes	prime
49	no	composite
51	no	composite
53	yes	prime
55	no	composite
57	no	composite
59	yes	prime
61	yes	prime
63	no	composite
65	no	composite
67	yes	prime
69	no	composite
71	yes	prime
73	yes	prime
75	no	composite
77	no	composite
79	yes	prime
81	no	composite
83	yes	prime
85	no	composite
87	no	composite
89	yes	prime
...	...	...

Significantly, the next odd integer, namely the composite number 91 or (7)(13), proves to be a counterexample. To show that $91|R_{90}$, note first that 7 is a divisor of R_6 in which case $7|R_{6(15)}$. By use of the fact that $13|R_6$ (easily shown), it follows that $13|R_{6(15)}$. Accordingly, $91|R_{90}$. As 91 is a deceptive prime, major questions of cardinality and frequency of encounter arise.

To establish that the set of deceptive primes is infinite, the concept of primitive divisors is needed. It can be shown that each repunit number R_x has a prime divisor which will not divide any smaller repunit. These prime divisors are called primitive and are nicely illustrated by such examples as "11 is a primitive divisor of R_2 and 37 is a primitive divisor of R_3." In particular, it can be shown for odd integers x greater than 3 that any two primitive divisors of R_x when multiplied yield a deceptive prime [3]. For example, 41 and 271, with a product of 11111, are primitive divisors of R_5 and thus, imply that $(41)(271)|R_{11110}$. Moreover, if a is a primitive divisor of R_x and b is a primitive divisor of R_{2x}, then ab is a deceptive prime. Since new deceptive primes can be found for each choice of R_x, it follows that the set of deceptive primes is infinite.

4. Explorations. The infinitude of the set of deceptive primes tells us little about their distribution. Nor does it reveal the probability of the primality of p on the basis of its being a divisor of R_{p-1}. Such a probability question is unanswered though it is much akin to the converse of Fermat's Little Theorem and its probable prime predicaments.

Interestingly, the cardinality of the set of repunit primes is today unknown. Obviously, if R_x is prime, then x itself must be prime. However, the converse fails [6]. For example,

$$\begin{gathered}
R_3 = (3)(37) \\
R_5 = (41)(271) \\
R_7 = (239)(4649) \\
R_{11} = (21649)(513239) \\
R_{13} = (53)(79)(265371653) \\
R_{17} = (2071723)(5363222357) \\
R_{29} = (3191)(16763)(43037)(62003)(77843839397).
\end{gathered}$$

This is somewhat of a variation on the converse situation above, yet it pinpoints a very challenging area of endeavor. In particular, for which values of prime x is R_x a prime number? Only five repunit primes are known today, these being R_2, R_{19}, R_{23}, R_{317}, and R_{1031}. Such a list is known to be complete for all subscripts x less than $10,000$. However, the more difficult question of whether or not there is a largest repunit prime is presently unanswered.

A subtle converse situation likewise arises here. Note again that if x is composite, then R_x is composite. However, if R_x is composite, does it follow that x is composite too? Actually, x may well be prime as illustrated in the table above. That is, R_5, R_7, R_{11}, R_{13}, and R_{17} are each composite, yet all subscripts are prime. Such prime subscripts illustrate what may be labeled as pseudo-composites. They suggest an interesting counterpart to false primes.

It can be shown that if x is a prime greater than 3, then any composite number R_x is a deceptive prime. As $x|R_{x-1}$, then $x|10R_{x-1}$. In other words, $x|R_x - 1$. Building on the theorem "$a|b$ implies $R_a|R_b$," it follows that $R_x|R_{(R_x-1)}$. For example, $R_{11}|R_{(R_{11}-1)}$ in which case R_{11} or (21649)(513239) is a deceptive prime. The cardinality of the set of composites R_x for which x is prime is here unresolved.

5. Conclusion. Again, consider the theorem "H_p implies C" where the hypothesis H_p contains the restriction that p is prime. Should the converse statement "C implies H_p" be false yet distinguished by hard-to-find counterexamples, the situation becomes right for fraudulent primes to appear. For example, if $2^n - 1$ is prime, then n is prime. Yet the primality of n may produce composites of the form $2^n - 1$ (e.g., $n = 11$). Such composite numbers $2^n - 1$ for which n is prime again provide a class of false primes. Admittedly, the subjective reference "hard-to-find counterexamples" is open to some debate. However, the reader is invited to find other instances of false primes by taking into account a seemingly scarce occurrence of composites as counterexamples in an appropriate converse setting.

Whereas the scarcity of pseudoprimes to the base 2 within the interval of the first 20 billion positive integers is now known, the counterpart for deceptive primes (those composites x which divide R_{x-1}) remains a challenge. Whether or not such a test provides a good probabilistic technique or Monte Carlo method for establishing primality is today a conjecture. Yet it identifies an intriguing search (one which is barely begun here) in the broad area of converses. It likewise provides in the process still another look at the concept of fraudulent number types, be they pseudoprimes, deceptive primes, or the false primes of some other fundamental relationship.

Note. A more extensive search for deceptive primes (those less than $20,000,000$) is now being completed (in cooperation with Timothy R. Ray). Such a determination of the relative scarcity of deceptive primes, the pseudoprime (base ten) connection, and a listing of key deceptive prime properties provide the focus of the search.

References

1. D. M. Burton, *Elementary Number Theory*, Allyn and Bacon, Inc., Boston, 1976.

2. R. L. Francis, "The Bursting of the Dam (Infinite Sets, Countable and Otherwise)," *Primus* 2 (1992), 183–191.

3. R. L. Francis, "Mathematical Haystacks," *The College Mathematics Journal*, 19 (1988), 240–246.

4. D. H. Lehmer, "Test for Primality by the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, 33 (1927), 327.

5. C. Pomerance, "Lecture Notes on Primality Testing and Factoring," *MAA Notes Number 4*, Mathematical Association of American, Washington D.C., 1984.

6. S. C. Yates, "Factors of Repunits," *Journal of Recreational Mathematics*, 3 (1970), 114–119.